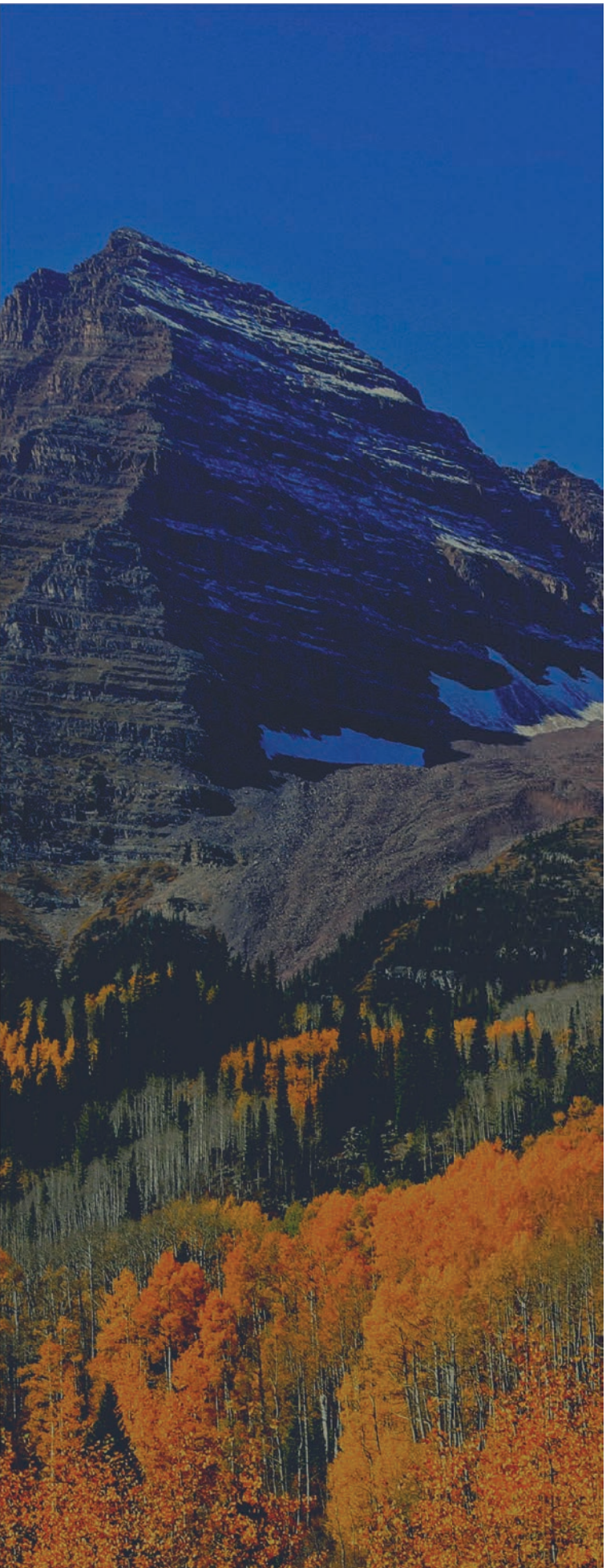
STOP Fraud Colorado

IDENTITY THEFT **REPAIR KIT**

Brought to you by the Colorado Attorney General's Office of Consumer Protection



CONSUMER PROTECTION IS OUR MISSION

Identity theft is one of the fastest-growing crimes in America, impacting millions of households each year. The threat is more pervasive, and the scams are more sophisticated than ever before. Identity thieves only need a few data points—like those found in widespread data breaches—and they can infiltrate your personal financial life, creating chaos. The damage can be life-altering.

Victims tell us that identity theft is about far more than the loss of money. It is about the loss of security and privacy. The destruction of hard-earned credit. The sense that someone who doesn't even know you now can assume your identity.

Our goal at the Colorado Attorney General's Office is to offer some useful tips to help you avoid becoming a victim of identity theft.

And because you can do everything right and still have your personal information stolen, we want to walk you through important steps to take if you do become a victim.

With knowledge comes power. We want Colorado residents to feel empowered when it comes to protecting themselves from identity theft. We hope you will find this guide a helpful resource.

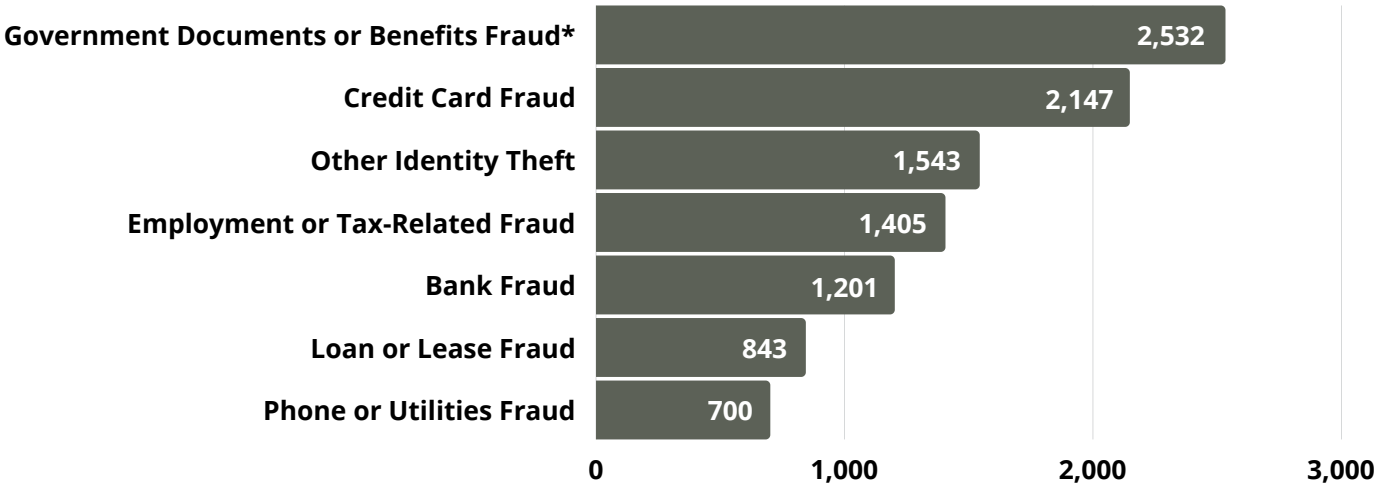
Table of Contents

Publication date: January 2021

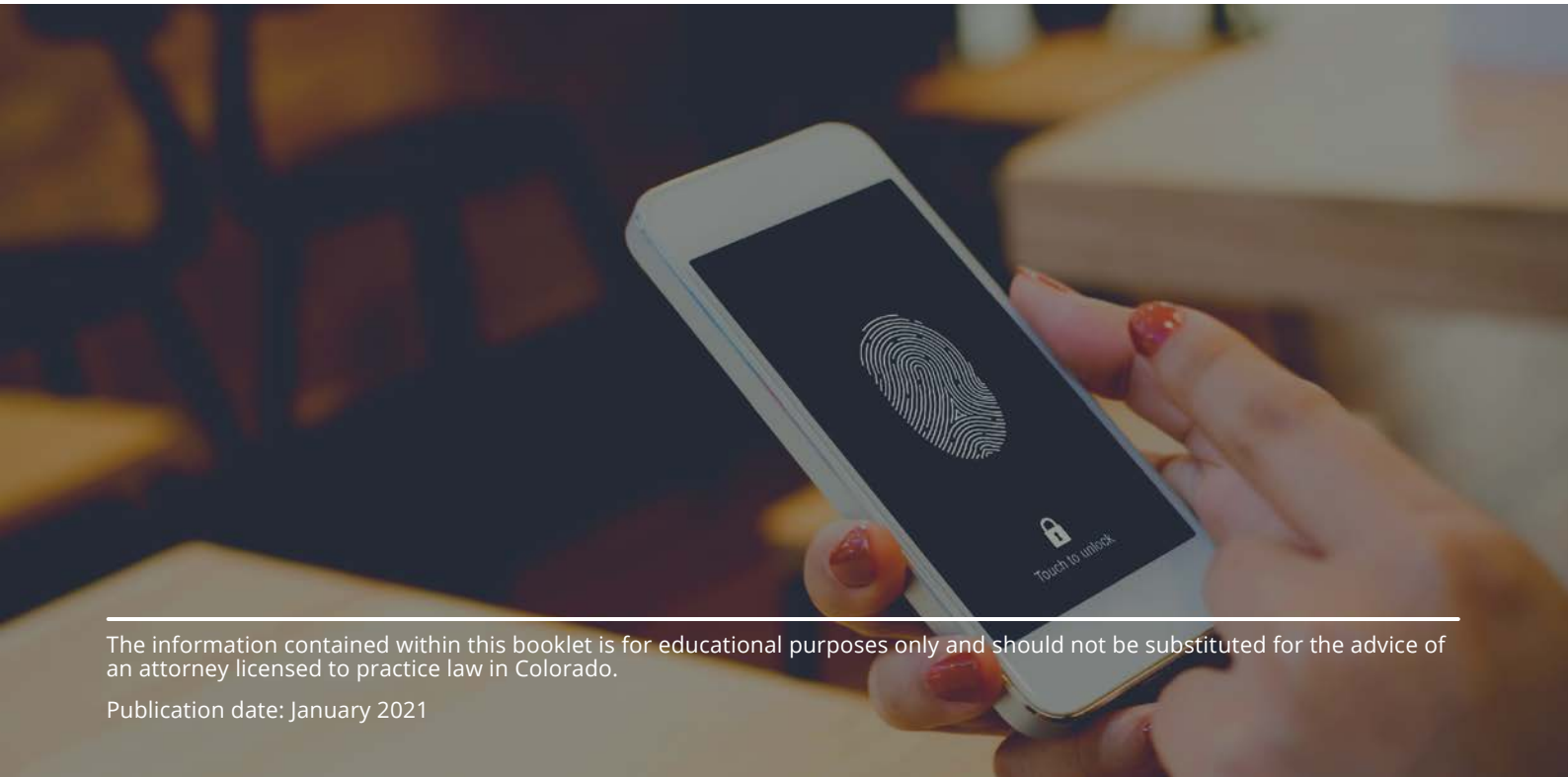
Introduction
What is Identity Theft?

Identity theft occurs when someone fraudulently uses your personal information to obtain credit, take out a loan, open accounts, get identification, or otherwise use your information in an unauthorized way.

Estimates from the Federal Trade Commission suggest that identity theft is on the rise. In fact, identity theft is the fastest growing crime in the country—a crime that affects Coloradans and their credit histories. According to the **FTC**, Colorado victims filed more than 8,709 identity theft complaints in 2020 involving the following types of fraud:



*Government Documents or Benefits Fraud includes the following subcategories of ID Theft: Tax- or Wage-Related Fraud, Government Benefits (Applied For/ Received), Other Government Documents (Issued/Forged), and Driver's License (Issued/Forged).



Publication date: January 2021

Emerging ID Theft Trends

Unemployment Insurance Fraud

A thief may use your information to file an unemployment insurance claim under your name.

You may discover that your information was used to file a fraudulent claim if you receive an unrequested ReliaCard or 1099G form in the mail, or if your employer informs you of a claim. If you believe that someone used your information to file a fraudulent unemployment insurance claim, you should:

- visit the Colorado Department of Labor and Employment (CDLE) website at **https://cdle.colorado.gov/fraud-prevention**
  - Follow steps to deactivate the ReliaCard, if you received one
  - File a fraud report
  - Specifically note if you received a 1099G form based upon a fraudulent filing

Once you file a fraud report, the CDLE will send you a letter confirming the fraudulent claim and identity theft. You can use this letter to take further steps in repairing your identity. CDLE will also send a corrected 1099G form so that your taxes are handled appropriately.

Income Taxes

Income tax identity theft usually occurs in one of two ways:

- Someone uses your Social Security number to get a job or as many have experienced lately, unemployment benefits. The employer or CDLE will report that person's earnings to the Internal Revenue Service (IRS). When you file your tax return, you won't include those earnings. But, IRS records will show you failed to report all your income and you can expect to get a letter from the IRS. CDLE is helping with the unemployment fraud by providing corrected reports to the IRS and you, but you may need to take steps if the employment scam occurs.
- Someone uses your Social Security number and files a tax return in your name before you file, they may get your refund. When you file your own return later, IRS records will show the first filing and refund, and you'll get a letter from the IRS.

If you think someone has misused your Social Security number to get a job, steal unemployment benefits, or steal a tax refund—or the IRS sends you a notice indicating a problem— contact the IRS immediately:

- at the number provided in the notice from the IRS;
- If instructed by the IRS, go to **IDVerify.irs.gov**;
- Complete IRS Form 14039, Identity Theft Affidavit
- Further information is available at **https://www.irs.gov/identity-theft-central**

Publication date: January 2021

Medical ID Theft

A thief may use your name or health insurance number to see a doctor, get prescription drugs, file claims with your insurance provider, or get other care. If the thief's health information is mixed with yours, your treatment, insurance and payment records, and credit report may be affected.

If you suspect an identity thief has used your medical information, you should:

- Get copies of your medical records. Under federal law, you have a right to know what's in your medical files.
- Contact each doctor, clinic, hospital, pharmacy, laboratory, health plan, and anywhere you believe the thief has used your information. For example, if a thief got a prescription in your name, ask for the record from the pharmacy that filled the prescription and the health care provider who wrote the prescription. You may need to pay a fee to get copies of your records.
- The medical provider or office that created the information must change any inaccurate or incomplete information in your files. They also should tell labs, other health care providers, and anyone else that might have gotten incorrect information. If an investigation doesn't resolve your dispute, ask that a statement of the dispute be included in your record.

Child ID Theft

Theft of a child's identity is growing rapidly, with some estimating that more than 10% of children have had their identity stolen. Because most children receive a Social Security number when they are born, and then don't apply for credit for many years, they become an enticing target for identity thieves. With a date of birth and a social security number, these thieves can apply for credit cards, loans, and other government services or benefits.

How do you know if your child's identity has been stolen?

- Your child begins to receive suspicious mail, like pre-approved credit cards and other financial offers normally sent to adults, in his or her own name.
- You try to open a financial account for him or her but find one already exists, or the application is denied because of a poor credit history.
- A credit report already exists in his or her name. If the child has one, he or she may have been targeted already, since only an application for credit, a credit account, or a public record starts the compilation of a consumer credit file.

A parent or guardian can check whether a minor child has a credit report if they think the child's information is at risk or if their child is approaching the age when they might first seek employment or credit of any kind. To get a minor child's credit report, a parent or guardian must contact the credit reporting companies and provide proof of identity and other documents, including a birth certificate and the child's social security card. Contact information for the three major credit reporting agencies is included at the back of this publication.

Publication date: January 2021

How do thieves get my personal or financial information?

Here are some of the ways identity thieves steal your personal and financial information:

- **Computer hackers** "breaking into" business or personal computers to steal private files and personal financial information, commonly known as a data breach.
- **Stealing your purse or wallet** to obtain social security cards, credit cards, driver's licenses, etc.
- **Stealing mail** being delivered to your home or left out for pick-up.
- **Diverting your mail** to another mailbox using a false "change of-address" request.
- **"Dumpster diving"—** thieves dig through dumpsters or garbage cans behind homes or businesses looking for discarded checks or bank statements, credit card or other account bills, medical records, pre-approved credit applications, etc.
- **"Shoulder surfing"—** thieves watch over your shoulder as you enter your PIN into an ATM.
- **"Pretext calls"—** thieves call to "verify" account information or to "confirm" an enrollment or subscription by having you repeat bank or credit card account numbers.
- **Using false or misleading Internet sites** to collect personal and financial information.
- **Purchasing personal information** from unscrupulous employees at companies with which you do business.
- **Burglarizing homes and businesses** looking for purses, wallets, computers and digital devices, files containing personal and financial information.
- **Phony e-mail or "pop-up" messages** known as click bait, phishing, and spam that appear to be from your credit card company, Internet Service Provider or other entity you do business with. These phony messages claim some problem with your account and direct you to another web site where you will be asked to supply credit card and other personal information or download malicious software or malware.
- **ATM skimming** involves the placement of a mechanical card reader over or into the actual card reader on an ATM machine. These fake card readers will capture your account number and possibly even your PIN code, which are then used to produce counterfeit credit or debit cards.

What do they do with it?

- **Collect government benefits in your name** by using your SSN to apply for a job or to obtain a tax return.
- **Drain your bank account** with electronic transfers, counterfeit checks, or your debit card.
- **Open a bank or credit account in your name** and write bad checks, make charges that never get paid off, which gets reflected on your credit report.
- **Use your name if they get arrested or for conducting illegal activity** such as drug purchases that could result in warrants being issued in your name or go on your permanent record.
- **Obtain a driver's license or a job** with your personal information.
- **Buy a car or property** and use your information and credit history to get a loan for it.
- **Obtain utility services in your name,** such as phone or Internet.

Publication date: January 2021

Identifying Identity Theft

Here are some warning signs that you may be the victim of identity theft:

- You are unexpectedly denied credit.
- You find charges on your credit card that you don't remember making.
- You suddenly stop receiving regular bank or credit card statements.
- Personal information, credit cards, ATM cards, checks, or IDs have been stolen from you.
- You have issues filing your taxes with the IRS.
- You suspect someone has fraudulently changed your mailing address.
- You find something wrong with your credit report, such as loans you didn't take out or accounts you don't remember opening.
- A debt collector calls about a debt you don't owe and didn't know about.
- You're arrested for a crime you didn't commit.

You could be the victim of identity theft without noticing any of these things happening to you. It is always a good idea to keep a careful eye out for anything out of the ordinary by ordering your free credit report at least once a year from **www.annualcreditreport.com**.

Protecting your passwords

- Do not use common numbers (like birth dates, phone numbers, or social security numbers) or commonly chosen words (child's name, maiden name, pet's name) as passwords or PINs.
- Never share your passwords or PIN numbers with anyone, not even a child or a spouse.
- Don't use the same passwords—or slight variations of the same passwords—for all of your computers and mobile devices, or for all of your online sites.
- Don't keep a written list of your passwords in your desk, filing cabinet, or anywhere a thief is likely to look.
- Choose strong passwords comprised of a combination of numbers, uppercase letters, lowercase letters, and, if possible, other characters.
- There are a variety of password manager tools that can generate completely random passwords and store them for you in an encrypted format.

Publication date: January 2021

What to Do Right Away if you are a Victim of Identity Theft

If you believe that you are a victim of identity theft, there are a number of important steps for you to take. Be prepared to document all unauthorized transactions and to be patient as the process can take a number of months.

Step 1: Call the companies where you know fraud occurred.

- Call the fraud department. Explain that someone stole your identity.
- Ask them to close or freeze the accounts. Then, no one can add new charges unless you agree.
- Change logins, passwords and PINS for your accounts.
- This is particularly important for all bank and credit card accounts where the financial institutions can take steps to further protect you and to try to address any losses that you may have incurred.

  You might have to contact these companies again after you have an FTC Identity Theft Report.

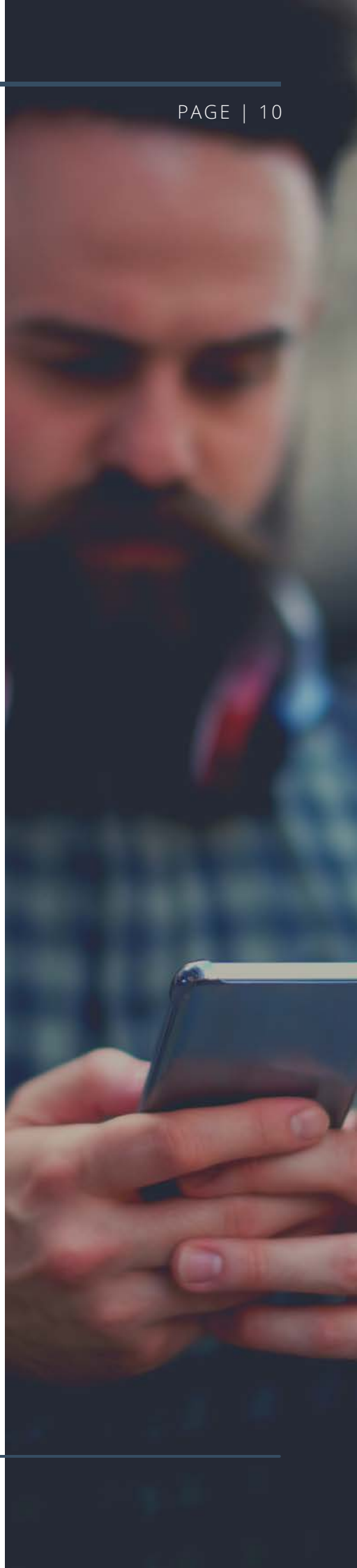
Step 2: Contact your homeowners insurance carrier.

Many, but not all, homeowners and renters insurance policies have protections in the event of identity theft. They may help you in taking steps to protect you from harm and may cover you for losses.

Step 3: Place a fraud alert and get your credit reports.

Place a free, one-year fraud alert by contacting one of the three credit bureaus. That company must tell the other two.

- **Experian.com/help**
  888-EXPERIAN (888-397-3742)
- **TransUnion.com/credit-help**
  888-909-8872
- **Equifax.com/personal/credit-report-services**
  800-685-1111
  - A fraud alert is free. It will make it harder for someone to open new accounts in your name. When you have an alert on your report, a business must verify your identity before it issues new credit in your name. You can renew the fraud alert after one year.
  - You'll get a letter from each credit bureau. It will confirm that they placed a fraud alert on your file.



Publication date: January 2021

Get your free credit reports from Equifax, Experian, and TransUnion. Go to **annualcreditreport.com** or call **1-877-322-8228**.

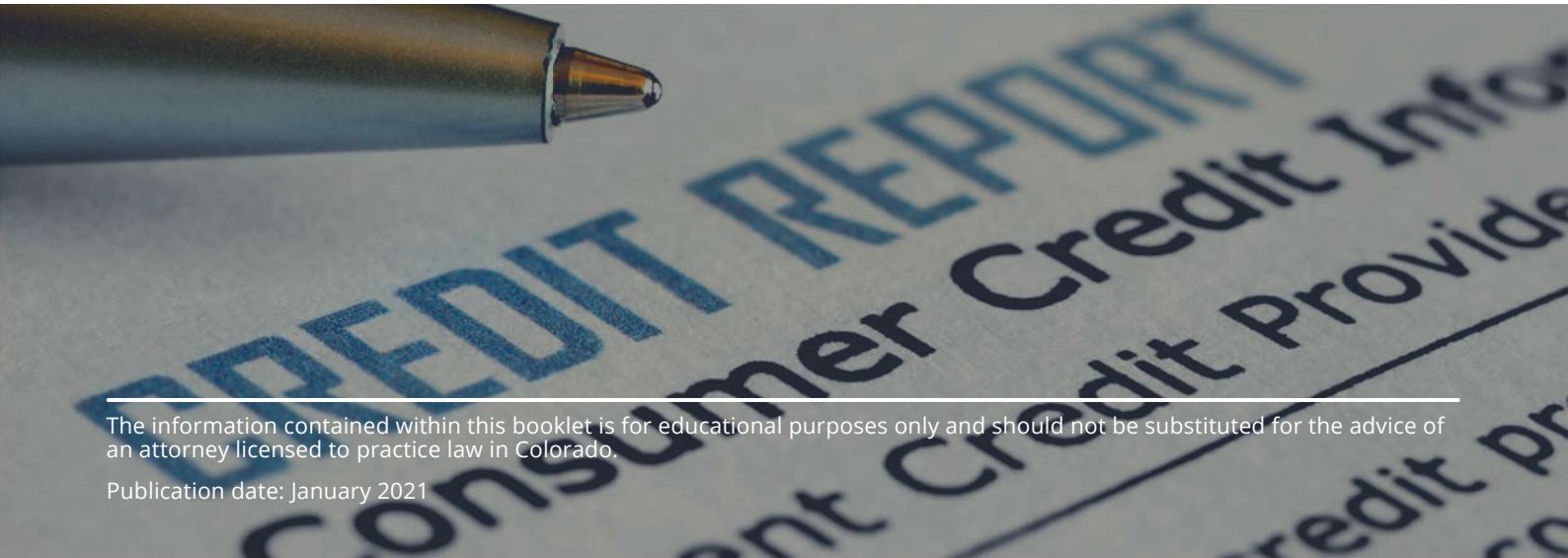
- Due to the pandemic, you can check your reports every week for free through April 2021 at **AnnualCreditReport.com**.
- Review your reports. Make note of any account or transaction you don't recognize. This will help you report the theft to the FTC and the police.

Step 4: Report identity theft to the FTC.

- Complete the **online form** or call **1-877-438-4338**. Include as many details as possible.
  - Based on the information you enter, **IdentityTheft.gov** will create your Identity Theft Report and recovery plan.
  - Your identity theft report proves to businesses that someone stole your identity. It also guarantees you certain rights.
- If you create an account, the FTC will walk you through each recovery step, update your plan as needed, track your progress, and pre-fill forms and letters for you.
- If you don't create an account, you must print and save your Identity Theft Report and recovery plan right away. Once you leave the page, you won't be able to access or update them.

Step 5: You may choose to file a report with your local police department.

- Go to your local police office with:
  - a copy of your FTC Identity Theft Report
  - a government-issued ID with a photo
  - proof of your address (mortgage statement, rental agreement, or utilities bill)
  - any other proof you have of the theft (bills, IRS notices, etc.)
  - **FTC's Memo to Law Enforcement [PDF]**
- Tell the police someone stole your identity and you need to file a report.
- Ask for a copy of the police report. You may need this to complete other steps.



Publication date: January 2021

What to Do Next

Take a deep breath and begin to repair the damage.

Close new accounts opened in your name.

- Now that you have an FTC Identity Theft Report, call the fraud department of each business where an account was opened.
  - Explain that someone stole your identity.
  - Ask the business to close the account.
  - Ask the business to send you a letter confirming that:
    - the fraudulent account isn't yours
    - you aren't liable for it
    - It was removed from your credit report
  - Keep this letter. Use it if the account appears on your report later on.
- The business may require you to send them a copy of your FTC Identity Theft Report or complete a special dispute form. This **sample letter** can help.
  - Write down who you contacted and when.

Remove bogus charges from your accounts

- Call the fraud department of each business.
  - Explain that someone stole your identity.
  - Tell them which charges are fraudulent. Ask the business to remove them.
  - Ask the business to send you a letter confirming they removed the fraudulent charges.
  - Keep this letter. Use it if this account appears on your credit report later on.
  - The business may require you to send them a copy of your FTC Identity Theft Report or complete a special dispute form. This **sample letter** can help.
- Write down who you contacted and when.

Correct your credit report.

- Write to each of the three credit bureaus. This **sample letter** can help.
  - Include a copy of your FTC Identity Theft Report and proof of your identity, like your name, address, and Social Security number.
  - Explain which information on your report came from identity theft.
  - Ask them to block that information.
    - **TransUnion.com**
      Fraud Victim Assistance Department
      P.O. Box 2000
      Chester, PA 19016
      1-800-680-7289
    - **Equifax.com**
      P.O. Box 105069
      Atlanta, GA 30348-5069
      1-800-525-6285
    - **Experian.com**
      P.O. Box 9554
      Allen, TX 75013
      1-888-397-3742

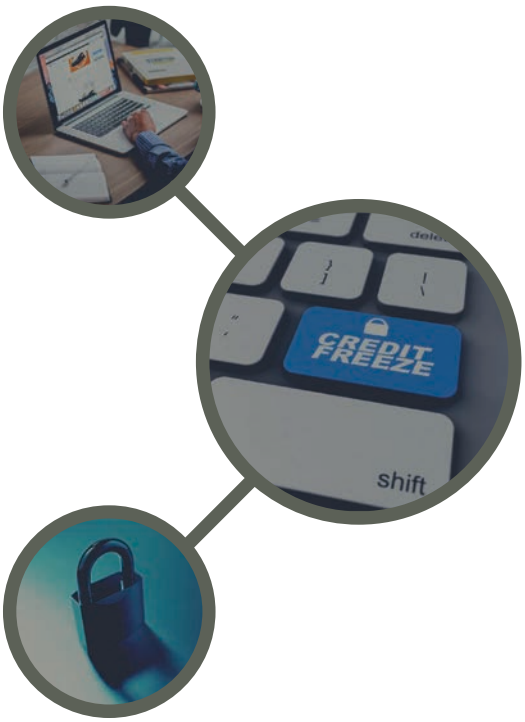
Publication date: January 2021

If someone steals your identity, you have the right to remove fraudulent information from your credit report. This is called blocking. Once the information is blocked, it won't show up on your credit report, and companies can't try to collect the debt from you. If you have an FTC Identity Theft Report, credit bureaus must honor your request to block this information.

If you don't have an FTC Identity Theft Report, you still can **dispute incorrect information** in your credit file. It can take longer, and there's no guarantee that the credit bureaus will remove the information.

Consider adding an extended fraud alert or credit freeze.

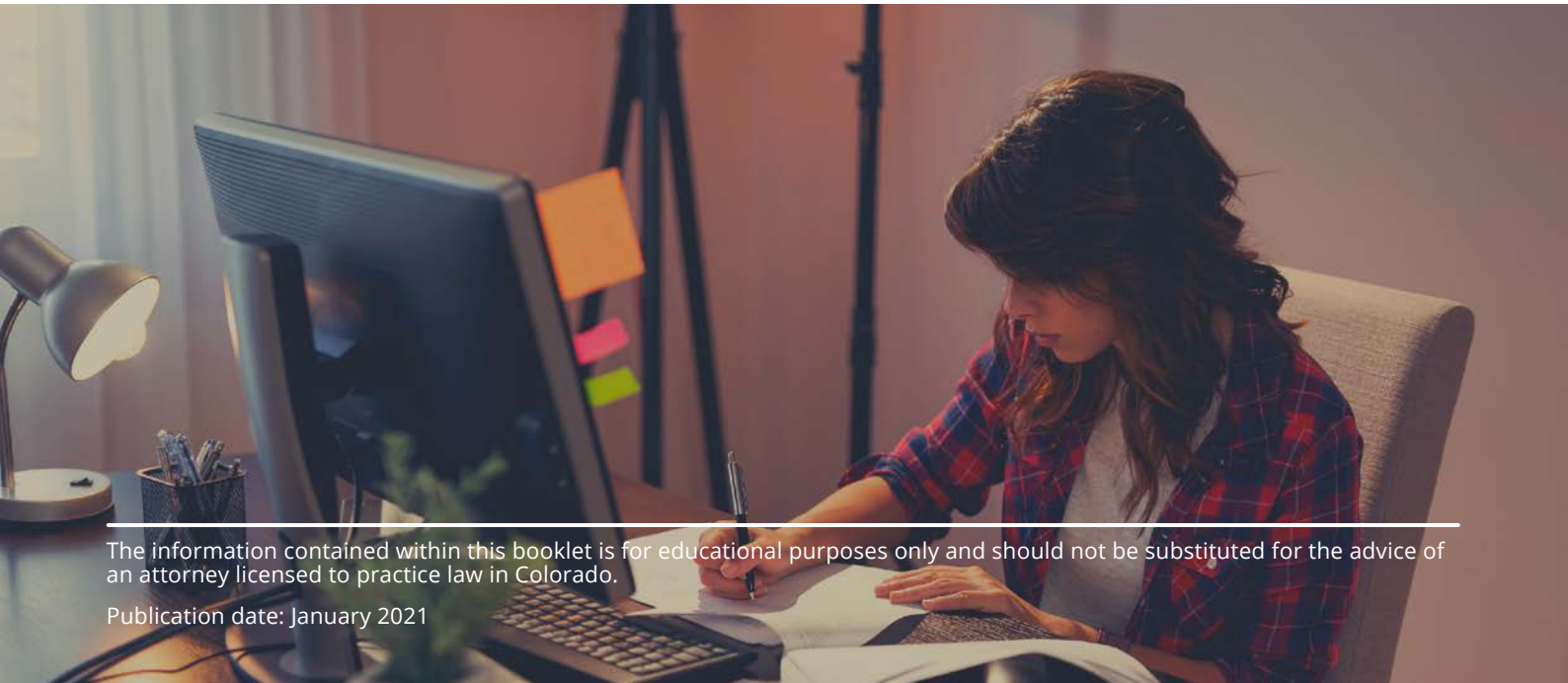
Extended fraud alerts and credit freezes can help prevent further misuse of your personal information. There are important differences. This chart can help you decide which might be right for you.



- **Extended Fraud Alert**
  - Lets you have access to your credit report as long as companies take steps to verify your identity.
  - Free to place and remove. Available if someone stole your identity.
  - Lasts for 7 years.
  - Set it by contacting each of the three credit bureaus:
    - Report that someone stole your identity. Request an extended fraud alert.
    - Complete any necessary forms and send a copy of your FTC Identity Theft Report.
- **Credit Freeze**
  - Stops all access to your credit report unless you lift or remove it.
  - Free to place and remove. Available to anyone.
  - Lasts until you lift or remove it.
  - Set it by contacting each of the three credit bureaus.

Review your credit reports often.

- Through April 2021, you can check your reports every week for free at **AnnualCreditReport.com**. This can help you spot any new fraud quickly.



Publication date: January 2021

Other Possible Steps

Depending on your situation, you might need to take additional steps.

Report a misused Social Security number.

- Social Security card lost or stolen? **Apply online** for free to get a replacement card.
- Do you think someone else is using your Social Security number for work? Review your Social Security work history by creating an account at **socialsecurity.gov/myaccount**. If you find errors, contact your **local SSA office**.

Stop debt collectors from trying to collect debts you don't owe.

- Write to the debt collector within 30 days of getting the collection letter. This **sample letter** can help.
  - Tell the debt collector someone stole your identity, and you don't owe the debt.
  - Send copies of your Identity Theft Report and any other documents that detail the theft.
- Contact the business where the fraudulent account was opened.
  - Explain that this is not your debt.
  - Tell them to stop reporting this debt to the credit bureaus.
  - Ask for information about the debt, and how it happened. The business must give you details if you ask. This **sample letter** can help.
  - For example, if someone opened a credit card in your name, ask for a copy of the application and the applicant's signature.
- If you haven't already, ask the credit bureaus to block information about this debt from your credit report.
  - The advice in **Disputing Errors on Credit Reports** can help you block fraudulent information from your credit reports.
  - Write down who you contacted and when. Keep copies of any letters you send.

Replace government-issued IDs.

- Social Security card lost or stolen? **Apply online** for free to get a replacement card.
- Driver's license lost or stolen? Contact the **nearest DMV branch** to report it.
  - The state might flag your license number in case someone else tries to use it, or they might suggest that you apply for a replacement license.
- Passport lost or stolen? Call the State Department at **1-877-487-2778** or TTY **1-888-874-7793**. If you want to replace the passport, you have several options:
  - If you are traveling within the next two weeks, make an appointment to apply in person at a **Passport Agency or Center**.
  - If you ***are not*** traveling within two weeks, submit Form **DS-11 [PDF]** and **DS-64 [PDF]** in person at an authorized **Passport Application Acceptance Facility**.

Publication date: January 2021

Clear your name of criminal charges.

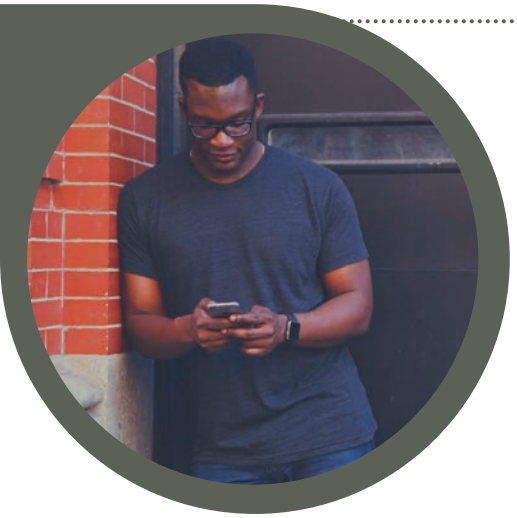
- If someone is arrested and uses your name or personal information, contact the law enforcement agency that arrested the thief. You may need to check court records to find out where the imposter was arrested.
  - File a report about the impersonation.
  - Give copies of your fingerprints, photograph, and identifying documents.
  - Ask the law enforcement agency to:
    - compare your information to the imposter's
    - change all records from your name to the imposter's name (if you know it)
    - give you a "clearance letter" or "certificate of release" to declare your innocence
  - Keep the clearance letter or "certificate of release" with you at all times.
  - Write down who you contacted and when.
- If a court prosecutes an identity thief using your name, contact the court where the arrest or conviction happened.
  - Ask the district attorney for records to help you clear your name in court records.
  - Provide proof of your identity.
  - Ask the court for a "certificate of clearance" that declares you are innocent.
  - Keep the "certificate of clearance" with you at all times.
- Consider hiring a criminal defense lawyer. The **American Bar Association** can help you find a lawyer.
- Ask the law enforcement agency that arrested the thief which information brokers buy their records.
  - Information brokers buy criminal records and sell information to employers and debt collectors.
  - Write to the brokers. Ask them to remove errors from your file.
- Write down who you contacted and when. Keep copies of any letters you send.

Steps for Certain Accounts

For certain types of accounts, you might have to contact additional offices.

Utilities

- If someone used your information to get cable, electric, water, or other similar services, contact the service provider.
  - Tell them someone stole your identity.
  - Ask them to close the account.
- For additional help, contact your **state Public Utility Commission** and explain the situation.
- Write down who you contacted and when. Keep copies of any letters you send.



Phones

- Contact the National Consumer Telecom and Utilities Exchange and request your NCTUE Data Report. Review it for any accounts you don't recognize.
  - **https://www.nctue.com/**
  - **1-866-349-5185**
- What is the NCTUE data report? The NCTUE data report is a record of all telecommunication, pay TV and utility accounts reported by exchange members, including information about your account history, unpaid accounts and customer service applications.
- If the service provider doesn't resolve the problem, file a complaint with the **Federal Communications Commission** at **1-888-225-5322** or TTY **1-888-835-5322**.

Publication date: January 2021

Government Benefits

- The specific circumstances related to unemployment benefits during the novel coronavirus pandemic are described above.
- Otherwise, contact the agency that issued the government benefit and explain that someone stole your identity. You can find local government agencies here.
  - For Social Security Benefits, contact the SSA Office of the Inspector General at **www.socialsecurity.gov/oig** or **1-800-269-0271**.
- Ask what you need to do to fix the problem.
- If you stopped receiving your benefits because of the identity theft, ask what you need to do to get them reinstated. You may need to appear in person or send something in writing.
- Make a note of who you contacted and when.

Checking accounts

- Do you think someone opened a checking account in your name? Order a free copy of your ChexSystems report, which compiles information about your checking accounts.
  - To get your report, contact ChexSystems at **1-800-428-9623**. Or visit their **website**.
  - Then contact every financial institution where a new account was opened. Ask them to close the accounts.
- If someone is writing bad checks against your account, contact your financial institution.
  - Ask them to stop payment on stolen checks and close your account.
  - Ask them to report the theft to its check verification system. The check verification system will tell businesses to refuse the stolen checks.
  - Also, contact any business that took the bad check. Explain that someone stole your identity. Act quickly, before they start collection action against you.
- You also can contact check verification companies. Report that your checks were stolen. Ask them to tell businesses to refuse the stolen checks.
  - Telecheck **1-800-710-9898**
  - Certegy **1-800-437-5120**
- If a business rejects your checks, ask the business for an explanation. The business must tell you what information led them to reject your check.
- Write down who you contacted and when. Keep copies of any letters you send.

Student loans

- Contact the school or program that opened the loan
  - Explain the situation.
  - Ask them to close the loan, and send you a letter that says you aren't responsible for the loan.
- If this is a federal student loan, contact the **U.S. Department of Education Office of Inspector General** hotline at **1-800-MISUSED (1-800-647-8733)**.

Publication date: January 2021

- If these steps don't resolve your situation, contact the U.S. Department of Education Federal Student Aid Ombudsman at **1-877-557-2575** or **online**.
- Write down who you contacted and when. Keep copies of any letters you send.

Apartment or House Rentals

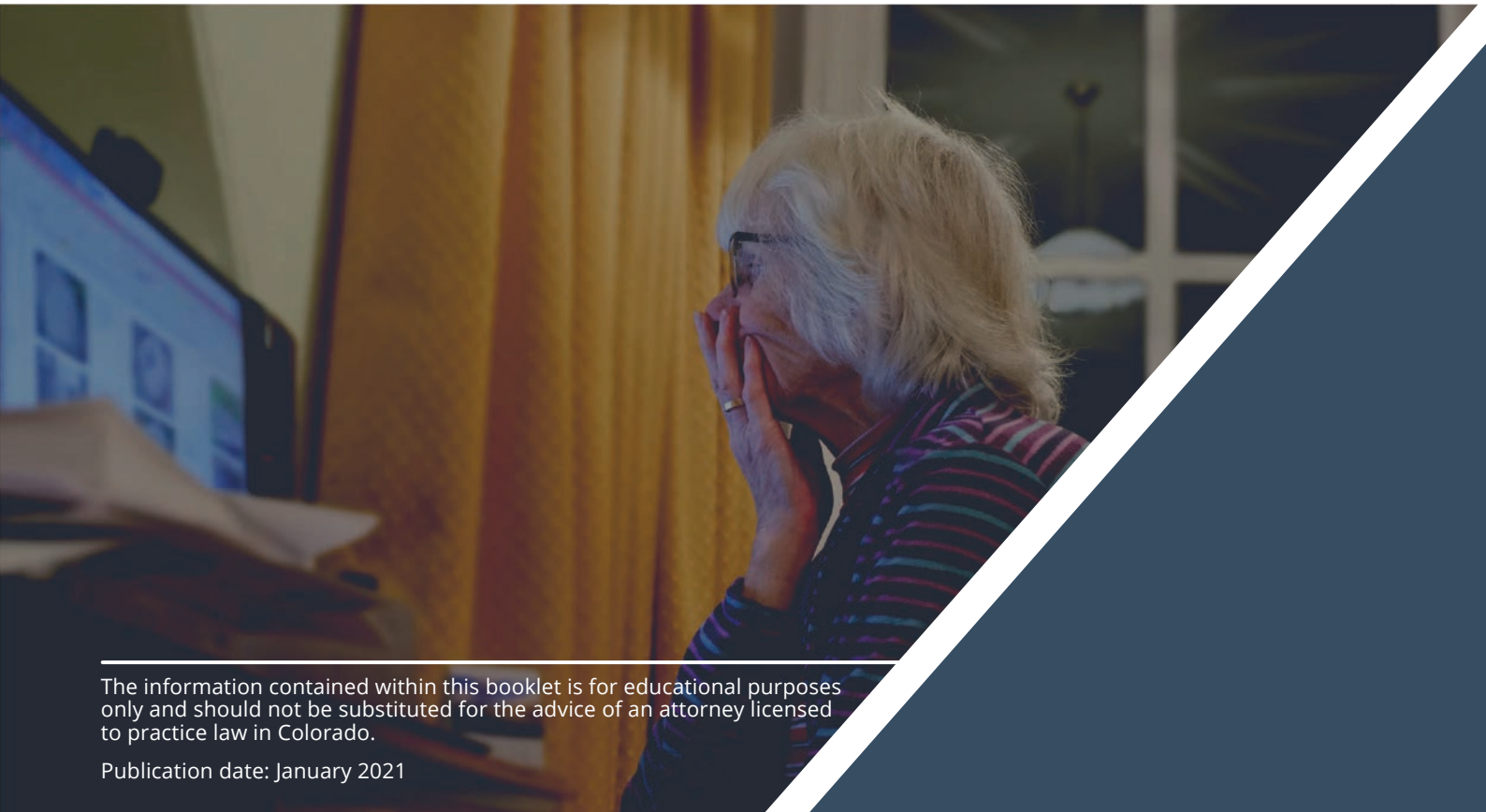
- Ask the landlord who rented the property to the identity thief what tenant history services they use. Contact those companies. Ask for a copy of your tenant history report, and ask what steps you need to take to correct fraudulent information in the report.
  - What's a tenant history report? There are several companies that collect and sell information about renters – such as how often a renter was late or if a renter has ever been evicted. If someone leased an apartment in your name, you'll want to correct any errors in your tenant history reports.
- Write down who you contacted and when. Keep copies of any letters you send.

Investment accounts

- Call your broker or account manager, and describe the situation.
- Write down who you contacted and when. Keep copies of any letters you send.

Bankruptcy filed in your name

- Write to the **U.S. Trustee** in the region where the bankruptcy was filed. Describe the situation and provide proof of your identity.
  - The U.S. Trustee Program refers cases of suspected bankruptcy fraud to the U.S. Attorneys for possible prosecution. The U.S. Trustee can't give you legal help, so you may need to hire an attorney.
- Consider hiring an attorney. The **American Bar Association** or a **local legal services** provider can help you find a lawyer.
  - An attorney can explain to the court that the bankruptcy filing was fraudulent.
- Write down who you contacted and when. Keep copies of any letters you send.



Publication date: January 2021

Do Not Give Up

Clearing up the problems caused by identity theft can be time intensive, as well as an emotional and frustrating process. It can take weeks, and even months, of work contacting creditors and credit reporting bureaus. DO NOT GIVE UP. Exercise all of your consumer rights and retain an attorney if creditors and credit reporting bureaus are not cooperating with your efforts to clear your name and credit.

Liability

To ensure that you don't end up paying hundreds or even thousands of dollars in fraudulent charges on your credit/debit cards made by an identity thief, the best course of action is to act quickly. The faster you act, the less liable you are for unauthorized charges.

Credit/debit cards

According to the Truth in Lending Act, your liability can be limited to $50 in unauthorized credit card charges per card if you notify your bank or card issuer immediately. Notification more than 2 days and less than 60 days after discovery will cap your losses at $500. After that (notification is more than 60 days after discovery) your liability might be unlimited. If an identity thief changed your mailing address, you must still send your letter within 60 days of when you were supposed to have received it (keep track of your bills!).

If your ATM or debit card is lost or stolen, report it as quickly as possible. If you report it within two business days, you are only responsible for $50 in unauthorized withdrawals or transfers. If you report it between two and 60 days after, you may be responsible for up to $500 in unauthorized withdrawals or transfers the thief may make. If you do not report it after 60 days, you can lose any money the thief withdraws or transfers from your account after the 60 days.

Security freeze

In order to prevent unauthorized access to your credit reports, Colorado law allows you to place a "security freeze" on those reports. Contact each consumer reporting bureau (Step 4 on page 14), **in writing by certified mail** and request that a freeze be placed on your account. You cannot be charged for the initial request. Once a freeze is in place, the bureau will not be able to release your credit report, or any information contained in the report, without your prior, express authorization. For more information about security freezes, including a list of those entities that will still be allowed to access your credit information, visit **https://stopfraudcolorado.gov/fraud-center/identity-theft.html**.

Checklist

Plan of action list

Because this is a lot of information to take in, we have provided you with a checklist to go through to make sure you have taken all the necessary steps after becoming an identity theft victim. Remember, you must complete all of these steps in a timely manner so that the identity theft does not get worse and to minimize your losses.

- [ ] Filed a police report.
- [ ] Filled out the Identity Theft Affidavit.
- [ ] Obtained a copy of your credit report.
- [ ] Identified errors, inquiries you did not know about, accounts you did not open, debts you did not know about, or anything else that seems wrong or out of place on your credit report.
- [ ] Placed a fraud alert on your credit report.
- [ ] Closed any accounts that might have been tampered with or opened without your knowledge or consent.
- [ ] Contacted a major credit bureau by phone and by writing to correct inaccurate information.
- [ ] Contacted the correct agencies to fix inaccurate information, close accounts, or report identity theft.
- [ ] Filed a complaint with the Federal Trade Commission.

Publication date: January 2021

Document list

Here is a list of documents you should have. You won't be able to keep the originals of some of the documents so it is very important that you make a copy for yourself. It is also a good idea to keep copies of the documents that prove you are an identity theft victim with you, such as a copy of your police report.

- [ ] Police report
- [ ] Identity Theft Affidavit
- [ ] Bills with fraudulent charges
- [ ] Documentation of accounts opened in your name without your consent
- [ ] Copies of letters sent to credit bureaus and creditors
- [ ] Copies of all letters to and from collection agencies

Tips on preventing Identity Theft

There are a number of things you can do to minimize the chances that you will become a victim of identity theft:

- **NEVER** provide personal identifying or financial information during a telephone call you did not initiate. Banks, credit card companies, telephone companies and other legitimate creditors do not call to "verify" account numbers or to ask for your social security number or other personal information.
- **NEVER** provide personal identifying or financial information over the telephone to anyone claiming to represent a contest or sweepstakes promotion. It is illegal to market a foreign lottery in the United States. These calls are always fraudulent.
- **NEVER** carry your social security card in your purse or wallet.
- **NEVER** have your social security number printed on your checks, driver's license or other financial documents. If a bank, health care provider or other entity uses your social security number for client or account identification, call or write that company and ask that a different identification number be issued.
- **NEVER respond to e-mail or "pop-up" messages on your computer claiming some problem with a credit card, Internet, or other account.** Promptly contact your real credit card company or ISP to verify that there are no problems with your account.
- **Use a "cross-cut" shredder** and get in the habit of shredding all personal or financial documents before placing them in the trash. Shred copies of bills and invoices after you have paid them, bank statements (including your canceled checks), investment or retirement account statements, pre-approved credit card or loan applications (especially those that come with a negotiable check attached), medical statements of any kind, and any other documents with information about you or your finances.
- **Password protect all credit card accounts that allow it.** Do not use common numbers or personal information (like birth dates or part of your social security number) or commonly chosen words (such as a child's, spouse's, or pet's name) for passwords.
- **Control access to your credit history.** Remove your name from mailing lists for pre-approved lines of credit by participating in the "Opt-Out" program. Call 1-888-5-"OPT OUT" (1-888-567-8688) or visit www.optoutprescreen.com to enroll. You will need to provide your social security number to verify that you are making the request, but this is a legitimate use of such information.
- **Be careful with your incoming and outgoing mail.** If you don't have a secure, locked mailbox, mail your bills from a curbside public mailbox or directly at your local post office. NEVER leave outgoing mail in an un-secured mailbox overnight. If you are planning on being away from home, arrange with your post office to hold your mail.
- **Arrange to pick up new checks at your bank.** NEVER have boxes of new checks delivered to your home (they do not fit in many mail slots so your postal carrier may leave them on your doorstep).
- **Take all credit card or ATM receipts with you after you pay for goods or services.** Do not just leave them behind or throw them away in the trash can. Destroy them in your cross-cut shredder when you get home.

Publication date: January 2021

- **Write to your bank, insurance company and other financial institutions you do business with and tell them not to share your customer information with unaffiliated third parties.** Under federal law, they are required to honor this request.
- **Remove your name from national direct mail advertising lists.**
  Send your name and address with a written request to:
  DMA Mail Preference Service ATTN: Dept. 12059580
  Direct Marketing Association
  P.O. Box 282 Carmel, NY 10512
- **To dramatically reduce telephone solicitations, sign up with the Colorado No-Call List.**
  Register on-line at **www.coloradonocall.com/** or by calling **1-800-309-7041**.
- Participate in the national no-call registry by going on-line at **https://www.donotcall.gov/register.html**.

Contacts

Colorado Attorney General's Office
www.coag.gov
www.stopfraudcolorado.gov
https://stopfraudcolorado.gov/fraud-center/identity-theft.html

Ralph L. Carr Colorado Judicial Center
1300 Broadway, 10th Floor
Denver, CO 80203
(720) 508-6000
Consumer Line: 1-800-222-4444

Federal Trade Commission
https://www.identitytheft.gov/

Consumer Response Center,
Room 130-B 600 Pennsylvania Avenue N.W.
Washington, D.C., 20580
1-877-ID-THEFT (1-877-438-4338)
1-866-653-4261 (TTY)

Major Credit Bureaus

Equifax:
www.equifax.com
P.O. Box 740241 Atlanta, GA 30374-0241
1-800-525-6285

Experian:
www.experian.com
P.O. Box 9532 Allen, TX 75013
1-888-EXPERIAN (397-3742)

TransUnion:
www.transunion.com
childidtheft@transunion.com
Fraud Victim Assistance Division
P.O. Box 6790
Fullerton, CA 92834-6790
1-800-680-7289

Publication date: January 2021

A free copy of your credit report is available from the website **https://www.annualcreditreport.com/index.action** or write to:

Central Source LLC
P.O. Box 105283
Atlanta, GA 30348-5283
or call: 1-877-322-8228
TDD: 1-877-730-4104

Major Check Verification Companies
To request a copy of your consumer report specifically about your checking account: Chex Systems, Inc. at 1-800-428-9623 or **https://www.chexsystems.com**

To request that your checks not be accepted by retailers: Certegy, Inc. (previously Equifax Check Systems) at 1-800-437-5120 TeleCheck at 1-800-710-9898 or 1-800-927-0188

Social Security Administration
https://www.ssa.gov/

SSA Fraud Hotline
P.O. Box 17768
Baltimore, MD 21235
SSA Fraud Hotline: 1-800-269-0271
1-866-501-2101 (TTY)

U.S. Postal Inspection Service
To find your local postal inspection office visit: **https://www.uspis.gov/**

Colorado Division of Motor Vehicles
Visit this website to find the DMV service center closest to you: **https://www.colorado.gov/dmv**

We Are Here to Help You!

Publication date: January 2021

Publication Date: January 2021